BaFin

Bundesanstalt für
Finanzdienstleistungsaufsicht

Aufsichtsmitteilung

Hinweise zur Umsetzung von DORA mit vereinfachtem IKT-Risikomanagementrahmen (Artikel 16 DORA) und IKT-Drittparteienrisikomanagement

Bankenaufsicht / Referat CTF 5 Grundsatz DORA, IKT-Risikomanagement und
IKT-Drittparteienrisikomanagement

Stand: August 2025

Inhaltsverzeichnis

I. Vorwort

Mit der Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor (Digital Operational Resilience Act – DORA), hat die Europäische Union eine finanzsektorübergreifende europäische Regulierung für die Themen digitale operationale Resilienz, IKT-Risiken und Cybersicherheit geschaffen. Die Verordnung ist am 16. Januar 2023 in Kraft getreten und wird seit dem 17. Januar 2025 angewendet. Darüber hinaus hat das Finanzmarktdigitalisierungsgesetz (FinmadiG) auf nationaler Ebene umzusetzende Regelungen geschaffen, die unter anderem den Anwendungsbereich, einschließlich des vereinfachten IKT-Risikomanagementrahmens nach Artikel 16 DORA, betreffen.

Das (vereinfachte) IKT-Risikomanagement und das solide Management des IKT-Drittparteienrisikos sind zwei übergreifende Kernelemente von DORA. Sie sollen Finanzunternehmen[1] einen Rahmen bieten, mit dem sie sowohl ihre IKT-Risiken als auch ihre IKT-Drittparteienrisiken systematisch identifizieren, bewerten und steuern können. Die Anforderungen an das IKT-Risikomanagement decken daher dem Grunde nach die Themen ab, die von der BaFin über die sektoralen aufsichtlichen Anforderungen an die IT (BAIT/VAIT/KAIT/ZAIT) adressiert werden bzw. wurden. Gleichwohl unterscheidet sich der methodische Ansatz der Regelwerke, was zu Herausforderungen bei der Umsetzung der DORA-Anforderungen führen kann.

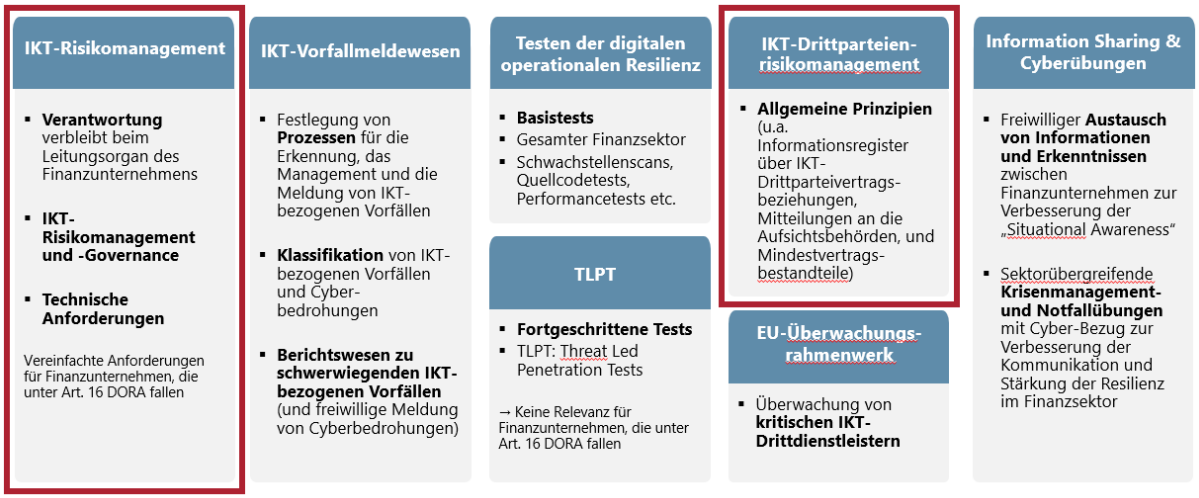
Diese Aufsichtsmitteilung richtet sich insbesondere an diejenigen von der BaFin beaufsichtigten Finanzunternehmen, die bisher unter die Anwendungsbereiche der Bankaufsichtlichen Anforderungen an die IT (BAIT) oder der Versicherungsaufsichtlichen Anforderungen an die IT (VAIT) gefallen sind – oder übergangsweise noch unter die BAIT fallen – und die Anforderungen an den vereinfachten IKT-Risikomanagementrahmen gemäß Artikel 16 DORA einzuhalten haben (siehe Abschnitt 1). Aufsichtsobjekte, die unter die Zahlungsdiensteaufsichtlichen oder Kapitalverwaltungsaufsichtlichen Anforderungen an die IT (ZAIT oder KAIT) fielen, werden von Artikel 16 DORA nicht erfasst.

Im Anschluss an die „Hinweise zur Umsetzung von DORA im IKT-Risikomanagement und IKT-Drittparteienrisikomanagement" aus Juni 2024 soll die vorliegende Aufsichtsmitteilung bei der Umsetzung der DORA-Anforderungen an den vereinfachten IKT-Risikomanagementrahmen (Kapitel II, Artikel 16 DORA) und das IKT-Drittparteienrisikomanagement (Kapitel V, Abschnitt I DORA) einschließlich der einschlägigen technischen Regulierungsstandards (RTS, Level 2)[2] unterstützen. Die weiteren Kapitel der DORA werden in diesem Zusammenhang nicht thematisiert, wie die nachfolgende Abbildung in einer Gesamtbetrachtung zeigt:

[1] Als Finanzunternehmen werden in diesem Dokument Finanzunternehmen im Sinne des Artikel 2 Absatz 2 DORA sowie alle Unternehmen, die im Rahmen der nationalen Anwendungsbereichserweiterung per FinmadiG unter DORA fallen, bezeichnet.

[2] Level 2 ist immer gemeinsam mit DORA (Level 1) zu betrachten. Die finalen Fassungen sind von der Europäischen Kommission im Amtsblatt der EU veröffentlicht.

Abbildung 1: Wesentliche Elemente in DORA



Die Umsetzungshinweise berücksichtigen den zum Zeitpunkt ihrer Veröffentlichung aktuellen Stand der folgenden, für diese Aufsichtsmitteilung relevanten, RTS:

- Delegierte Verordnung (EU) 2024/1774 der Kommission vom 13. März 2024 zur Ergänzung der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Festlegung der Tools, Methoden, Prozesse und Richtlinien für das IKT-Risikomanagement und des vereinfachten IKT-Risikomanagementrahmens (nachfolgend „RTS RMF“)

- Delegierte Verordnung (EU) 2025/532 der Kommission vom 24. März 2025 zur Ergänzung der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Präzisierung der Aspekte, die ein Finanzunternehmen bei der Untervergabe von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen bestimmen und bewerten muss (nachfolgend „RTS SUB“)

In den Umsetzungshinweisen wird der Grundsatz der Verhältnismäßigkeit – auch als Proportionalitätsprinzip bezeichnet – nicht explizit ausgeführt. Dieser ist in Artikel 4 DORA für die Kapitel II, III, IV und V, Abschnitt I normiert. Damit wird sichergestellt, dass Finanzunternehmen bei der Anwendung von DORA risikobasiert vorgehen können. Die in einzelnen Artikeln enthaltenen Ausnahmen für Kleinstunternehmen werden ebenfalls nicht erläutert.

Ebenso wird auf die Definitionen des Artikel 3 DORA in der Analyse nur bei Relevanz Bezug genommen. Eine vergleichbare Liste von definierten Schlüsselbegriffen finden sich weder in den BAIT noch in den VAIT.

Die Umsetzungshinweise stellen keine verbindliche Auslegung der BaFin und auch keine Auslegungen im Rahmen der Fragen- und Antwort-Prozesse (Q&As) der drei Europäischen

Aufsichtsbehörden[3] (Europäische Behörde für das Versicherungswesen und die betriebliche Altersversorung, European Insurance and Occupational Pensions Authority (EIOPA), Europäische Bankenaufsichtsbehörde, European Banking Authority (EBA) und Europäische Wertpapier- und Marktaufsichtsbehörde, European Securities and Markets Authority (ESMA)) dar.

[3] Beantwortete Fragen können entweder auf den einzelnen Seiten der ESAs eingesehen werden (EIOPA Search QAs - European Union (europa.eu), EBA Search for Q&As | European Banking Authority (europa.eu), ESMA Search a question | European Securities and Markets Authority (europa.eu)) oder in dem Dashboard der ESAs für Joint-Q&As: joint Q&As (europa.eu)).

II. Umsetzungshinweise

Die folgenden Umsetzungshinweise für die Implementierung der Anforderungen von DORA an den vereinfachten IKT-Risikomanagementrahmen und das IKT-Drittparteienrisikomanagement werden unterteilt in die Abschnitte Anwendungsbereich, Governance und Organisation, Informationsrisiko- und Informationssicherheitsmanagement, IT-Betrieb, (IKT-)Geschäftsfortführung, IT-Projektmanagement und Anwendungsentwicklung, IKT-Drittparteienrisikomanagement, Operative Informationssicherheit und Identitäts- und Rechtemanagement.

Insgesamt ist festzuhalten, dass die Anforderungen des vereinfachten IKT-Risikomanagementrahmens (Artikel 16 DORA) im Vergleich zu den BAIT/VAIT geringer ausfallen. Hinsichtlich des IKT-Drittparteienrisikomanagements sind die Unterschiede weniger umfangreich. Darüber hinaus enthält DORA aufgrund seines Fokus auf die digitale operationale Resilienz Anforderungen, die sich nicht in den BAIT/VAIT[4] wiederfinden.

Beaufsichtigte Unternehmen, die nicht unter den Anwendungsbereich von DORA fallen, sind darauf hinzuweisen, dass Maßnahmen zum angemessenen Umgang mit IKT-/Cyberrisiken im Rahmen der ordnungsgemäßen Geschäftsorganisation in jedem Fall zu treffen sind.

1. Anwendungsbereich

Gemäß Artikel 16 Absatz 1 Unterabsatz 1 DORA haben bestimmte Finanzunternehmen nicht den regulären IKT-Risikomanagementrahmen der Artikel 5 bis 15 DORA anzuwenden. Stattdessen gelten für sie die Anforderungen des vereinfachten IKT-Risikomanagementrahmens gemäß Artikel 16 DORA.

Der Anwendungsbereich des Artikel 16 DORA ergibt sich zum einen direkt aus Artikel 16 i.V.m. Artikel 3 DORA und den dort zitierten sektoralen Vorschriften: Von der Regelung des Artikel 16 Absatz 1 Unterabsatz 1 DORA sind in Deutschland nur die kleinen und nicht verflochtenen Wertpapierinstitute (kleine Wertpapierinstitute gemäß Artikel 3 Nr. 34 DORA) sowie die kleinen Einrichtungen der betrieblichen Altersversorgung[5] (kleine EbAV gemäß Artikel 3 Nr. 53 DORA) erfasst.[6] Für die Anwendung des IKT-Drittparteienrisikomanagements gemäß Artikel 28–30 DORA gibt es keine vergleichbare Ausnahmeregelung.

Zum anderen hat der nationale Gesetzgeber im FinmadiG den Anwendungsbereich der DORA auf bestimmte Finanzunternehmen des Banken- und Versicherungssektors erweitert und diese verpflichtet, den vereinfachten IKT-Risikomanagementrahmen des Artikel 16 DORA

[4] Aus Gründen der besseren Lesbarkeit und einhergehend mit der Übergangsfrist zu der weiteren Anwendung der BAIT für bestimmte Finanzunternehmen im Gegensatz zu den VAIT wird insgesamt das Präsens verwendet.
[5] In Zusammenhang mit dem Anwendungsbereich der Verordnung ist Artikel 2 Absatz 3 lit. c DORA zu beachten: Für Einrichtungen der betrieblichen Altersversorgung, die Altersversorgungssysteme mit insgesamt weniger als 15 Versorgungsanwärtern betreiben, gilt DORA nicht.
[6] Von den Möglichkeiten in der Zahlungs- und E-Geld-Richtlinie, Ausnahmen festzulegen, hat Deutschland keinen Gebrauch gemacht. Von der CRD ausgenommene Institute, auf die der Artikel 2 Absatz 4 DORA Bezug nimmt, sind die Landesförderbanken und die Kreditanstalt für Wiederaufbau (KfW) durch das FinmadiG dem regulären IKT-Risikomanagementrahmen nach Artikel 5-15 DORA unterworfen worden.

anzuwenden. Durch § 293 Absatz 5 Versicherungsaufsichtsgesetz (VAG) neue Fassung fallen Versicherungsholdings im Sinne des § 7 Nr. 31 VAG und im Sinne des § 293 Absatz 4 VAG unter Artikel 16 DORA.

Anknüpfend an den Institutsbegriff des § 1 Absatz 1b KWG verpflichtet § 1a Absatz 2a KWG neue Fassung nunmehr alle Institute, die nicht schon nach Artikel 2 DORA unter den Anwendungsbereich der Verordnung fallen, DORA ab dem 1. Januar 2027 anzuwenden.[7] Für sie sind bis dahin weiter die BAIT einzuhalten, die erst mit Ablauf des 31. Dezember 2026 außer Kraft treten.

Von dieser Regelung sind insbesondere Bürgschaftsbanken, Finanzdienstleistungsinstitute (beispielsweise Finanzierungsleasing- und Factoringinstitute, Kryptowertpapierregisterführer), Wohnungsunternehmen mit Spareinrichtung und Drittstaatenzweigstellen nach § 53 KWG erfasst.

Tabelle 1: Anwendung von DORA nach Rechtsquelle und Art des umzusetzenden IKT-Risikomanagementrahmens

IKT-Risikomanagementrahmen	Anwendung gemäß DORA	Anwendung gemäß FinmadiG
Artikel 5-15 DORA	Artikel 2 DORA mit Ausnahme des Artikel 16 Absatz 1 Unterabsatz 1 DORA	*KfW* (§ 1 Absatz 1 S. 1 Nr. 4, § 2 Nr. 8, § 3 Nr. 16-18 KfWV) *Landesförderbanken* (§ 1a Absatz 2 KWG)
Artikel 16 DORA	*Kleine Wertpapierinstitute* (Artikel 16 Absatz 1 i.V.m. Artikel 3 Nr. 34 i.V.m. Nr. 33 DORA) *Kleine EbAV* (Artikel 16 Absatz 1 i.V.m. Artikel 3 Nr. 53 i.V.m. Nr. 52 DORA)	*Versicherungsholdings* (§ 293 Absatz 5 i.V.m. Absatz 4 und § 7 Nr. 31 VAG) *Nicht-CRR-Kreditinstitute* (§ 1a Absatz 2a, § 65a Absatz 3 KWG)

2. Governance und Organisation

In diesem Abschnitt werden die Anforderungen der Artikel 16 Absatz 1 und 2 DORA sowie Artikel 28 RTS RMF an die Governance und Organisation des vereinfachten IKT-Risikomanagementrahmens in DORA denen der Kapitel IT-Strategie (Kapitel 1) und IT-Governance (Kapitel 2) der BAIT/VAIT gegenübergestellt.

Eine IT-Strategie, wie sie in Kapitel 1 BAIT/VAIT gefordert wird, ist im vereinfachten IKT-Risikomanagementrahmen nicht spezifiziert. Ebenso ist keine Strategie für die digitale operationale Resilienz vorgesehen, wie sie der reguläre IKT-Risikomanagementrahmen fordert.

[7] Gemäß § 65a Absatz 3 KWG ist § 1a Absatz 2a ab dem 1. Januar 2027 anzuwenden. Die Anforderungen an das Meldewesen nach Kapitel III der Verordnung (EU) 2022/2554 sind seit dem 17. Januar 2025 anzuwenden.

Der vereinfachte IKT-Risikomanagementrahmen fokussiert in der Governance und Organisation auf das wirksame und umsichtige Management der IKT-Risiken zur Stärkung der digitalen operationalen Resilienz des einzelnen Finanzunternehmens. Hierfür ist ein interner Governance- und Kontrollrahmen vorgesehen. Im Vergleich zu den BAIT/VAIT sind diese Anforderungen allerdings weniger detailliert.

Insbesondere im Vergleich zum regulären IKT-Risikomanagementrahmen ist die operative Informationssicherheit im vereinfachten IKT-Risikomanagementrahmen stärker betont.

Ein weiterer Unterschied zeigt sich auch in der Konkretisierung der Aufgaben des Leitungsorgans, die im Vergleich zu BAIT/VAIT stärker betont werden.

2.1 Keine Strategie für die digitale operationale Resilienz gefordert

Der vereinfachte IKT-Risikomanagementrahmen sieht, im Gegensatz zu der in den BAIT/VAIT geforderten IT-Strategie, keine Strategie(n) vor (siehe auch Abschnitt 7.2). Die Anforderungen an die IT-Strategie aus den BAIT/VAIT, also der funktionalen, übergreifenden und breit angelegten Strategie zur gesamten IT, haben daher keine Entsprechung. Allerdings finden sich bestimmte Inhalte, die BAIT/VAIT in der IT-Strategie fordern, im vereinfachten IKT-Risikomanagementrahmen als Teil der allgemeinen, nicht strategiebezogenen Anforderungen wieder. So wird beispielsweise die strategische Entwicklung der IT-Aufbau- und IT-Ablauforganisation (Kapitel 1.2 lit. a BAIT/VAIT) als Anforderung an die Organisation unterhalb der Strategieebene abgebildet (Artikel 16 Absatz 1 lit. a DORA i.V.m. Artikel 28 Absatz 1 und 2 lit. b RTS RMF). Aussagen zum (IT-)Notfallmanagement, wie sie in der IT-Strategie aufgeführt sind, sind als Anforderungen zur (IKT-)Geschäftsfortführung Teil des vereinfachten IKT-Risikomanagementrahmens (siehe Abschnitt 5) und gehören unter anderem hinsichtlich der (IKT-)Geschäftsfortführungspläne zu den Aufgaben des Leitungsorgans (siehe Abschnitt 2.3).

Die Zuordnung gängiger Standards (Kapitel 1.2 lit. b BAIT/VAIT) zur Umsetzung der Informationssicherheitsanforderungen aus der IT-Strategie findet sich ebenfalls nicht deckungsgleich im vereinfachten IKT-Risikomanagementrahmen wieder. Allerdings legt auch die Verordnung, deutlich weniger prominent, in Erwägungsgrund 2 zum RTS RMF und spezifisch bei den Anforderungen zur Zugangskontrolle (Artikel 33 Absatz 1 lit. d RTS RMF) die Berücksichtigung von gängigen Standards beziehungsweise führenden Praktiken nahe und bleibt in seinen Anforderungen und deren Umsetzung durch die Finanzunternehmen ebenfalls standardneutral.

Kapitel 1.2 lit. c BAIT/VAIT befasst sich mit den Zielen, Zuständigkeiten und der Einbindung der Informationssicherheit in die Organisation. Hingegen sind im vereinfachten IKT-Risikomanagementrahmen durch das Leitungsorgan für alle IKT-bezogenen Funktionen klare Aufgaben und Zuständigkeiten sowie Ziele für die Informationssicherheit festzulegen (Artikel 28 Absatz 2 lit. b und c RTS RMF).

Die strategische Entwicklung der IT-Architektur (Kapitel 1.2 lit. d BAIT/VAIT) findet keine Entsprechung im vereinfachten IKT-Risikomanagementrahmen. Ebenso wenig findet sich die Anforderung der DOR-Strategie an die IKT-Referenzarchitektur (Artikel 6 Absatz 8 lit. d DORA) aus dem regulären IKT-Risikomanagementrahmen inklusive

Erläuterung etwaiger Änderungen, die für die Erreichung spezifischer Geschäftsziele erforderlich sind, im vereinfachten IKT-Risikomanagementrahmen wieder.

Auch wenn DORA eine IT-Strategie im Sinne der BAIT/VAIT nicht fordert, kann sich ihr Fortbestand, sowohl als mögliches Bindeglied zwischen Geschäftsstrategie und dem vereinfachten IKT-Risikomanagementrahmen als auch vor dem Hintergrund sektoraler Anforderungen an Strategien in der Geschäftsorganisation, als empfehlenswert und sinnvoll erweisen.

2.2 Erfordernis eines IKT-spezifischen internen Governance- und Kontrollrahmens

Der interne IKT-Governance- und Kontrollrahmen bildet im vereinfachten IKT-Risikomanagementrahmen den Rahmen für ein wirksames und umsichtiges Management von IKT-Risiken. Zu beachten ist dabei, dass die allgemeinen, nicht IKT-spezifischen Governance-Anforderungen aus den sektoralen Regelungen bestehen bleiben.

DORA adressiert die Governance des vereinfachten IKT-Risikomanagementrahmens, d. h. das wirksame und umsichtige Management der IKT-Risiken und als dessen Folge die Stärkung der Resilienz des jeweiligen Finanzunternehmens (Artikel 28 Absatz 1 RTS RMF). In den BAIT/VAIT ist der Fokus etwas anders gefasst und liegt insbesondere auf der Informationssicherheit und den damit einhergehenden Governance-Anforderungen.

Auch im vereinfachten IKT-Risikomanagementrahmen ist eine Risikogesamtsicht erforderlich, da das IKT-Risikomanagement in das allgemeine Risikomanagement des Finanzunternehmens einbezogen ist (Artikel 16 lit. a und c DORA, Artikel 28 Absatz 2 lit. a RTS RMF). Wie auch die BAIT/VAIT (vgl. Vorbemerkung Kapitel 4.2 VAIT, Kapitel 4.2 BAIT/VAIT) betont DORA in diesem Zusammenhang die Letzt- sowie die Gesamtverantwortung des Leitungsorgans (Artikel 28 Absatz 2 lit. a RTS RMF).

DORA fordert im vereinfachten IKT-Risikomanagementrahmen eine angemessene Trennung und die Unabhängigkeit von Kontrollfunktionen und internen Revisionsfunktionen (Artikel 28 Absatz 4 RTS RMF). Die BAIT/VAIT fordern allgemein die Vermeidung von Interessenkonflikten und unvereinbaren Tätigkeiten in der IT-Aufbau- und IT-Ablauforganisation (Kapitel 2.4/2.7 BAIT/VAIT). Bei der organisatorischen Ausgestaltung macht DORA beim vereinfachten IKT-Risikomanagementrahmen keine detaillierten Vorgaben. Gemäß Artikel 28 Absatz 2 lit. b RTS RMF sind für alle IKT-bezogenen Funktionen klare Aufgaben und Zuständigkeiten durch das Leitungsorgan festzulegen. Allgemeine sektorale Governance-Vorschriften sind zu beachten.

Die Berücksichtigung des Stands der Technik und der zukünftigen Bedrohungslage (Kapitel 2.3/2.4 BAIT/VAIT) sind auch im vereinfachten IKT-Risikomanagementrahmen vorhanden, wenngleich unter anderen Begrifflichkeiten (vgl. unter anderem Erwägungsgrund 48 DORA sowie Erwägungsgrund 2 RTS RMF, Artikel 31 Absatz 3, Artikel 32, Artikel 34 lit. h und i, Artikel 36 Absatz 1, Artikel 39 Absatz 1 lit. j, Artikel 41 Absatz 2 lit. a sublit. ii RTS RMF).

Ein wesentlicher Unterschied im Vergleich zum regulären IKT-Risikomanagementrahmen ist, dass der vereinfachte IKT-Risikomanagementrahmen keine IKT-Risikokontrollfunktion vorsieht (siehe Artikel 6 Absatz 4 DORA).

2.3 Konkretisierung der Aufgaben des Leitungsorgans

DORA konkretisiert im vereinfachten IKT-Risikomanagementrahmen die Anforderungen und Aufgaben an das Leitungsorgan (siehe insbesondere Artikel 28 Absatz 2 RTS RMF). Dadurch wird dessen Verantwortung hervorgehoben und dessen Rolle im Kontext der Governance und Organisation gestärkt. Ähnliche Anforderungen finden sich in den BAIT/VAIT als Aufgabe der Geschäftsleitung an spezifischen Punkten (unter anderem IT-Strategie, Regelungen zur IT-Aufbau- und IT-Ablauforganisation, Steuerung IT-Betrieb, Informationsrisikomanagement, Informationssicherheitsleitlinie, Informationssicherheitsmanagement, Untersuchung Informationssicherheitsvorfälle, IT-Projektmanagement), sind aber weniger konkret.

Das Finanzunternehmen stellt unter dem vereinfachten IKT-Risikomanagementrahmen sicher, dass sein Leitungsorgan:

- die Gesamtverantwortung dafür trägt, dass der vereinfachte IKT-Risikomanagementrahmen im Einklang mit der Risikobereitschaft und der Geschäftsstrategie des Finanzunternehmens steht und IKT-Risiken in diesem Zusammenhang berücksichtigt werden (Artikel 28 Absatz 2 lit. a RTS RMF);

- gemäß Artikel 28 Absatz 2 lit. c RTS RMF die Ziele für die Informationssicherheit und die IKT-Anforderungen festlegt, und die dafür notwendigen Verfahren, IKT-Protokolle und Tools ermittelt und implementiert (Artikel 28 Absatz 2 lit. g RTS RMF). Damit ist das Leitungsorgan verpflichtet, sich mit den Zielen der Informationssicherheit auseinanderzusetzen, auch wenn es die in Artikel 29 RTS RMF geforderte Informationssicherheitsleitlinie nicht genehmigen muss;

- die in Artikel 28 bis 40 RTS RMF vorgesehenen Maßnahmen sowie die Informationssicherheitsleitlinie gemäß Artikel 29 RTS RMF festlegt und umsetzt, um das IKT-Risiko, dem das Finanzunternehmen ausgesetzt ist, zu ermitteln, zu bewerten und zu managen (Artikel 28 Absatz 2 lit. f RTS RMF);[8]

- die in Artikel 30 Absatz 1 RTS RMF genannte Klassifizierung der IKT- und Informationsassets des Finanzunternehmens, die Liste der ermittelten Hauptrisiken und die zugehörigen Richtlinien genehmigt, überwacht und überprüft (Artikel 28 Absatz 2 lit. d i RTS RMF);

- die in Artikel 16 Absatz 1 lit. f DORA aufgeführten (IKT-)Geschäftsfortführungspläne, Gegen- und Wiederherstellungsmaßnahmen sowie die Business-Impact-Analyse (vgl. Artikel 39 Absatz 1 RTS RMF) genehmigt, überwacht und überprüft (Artikel 28 Absatz 2 lit. d sublit. ii i.V.m. Artikel 29 und 30 RTS RMF).
  Artikel 40 Absatz 3 RTS RMF sieht eine Meldung an das Leitungsorgan über Mängel vor,

[8] In der deutschen Sprachversion des RTS RMF ist die Übersetzung aus dem Englischen in Artikel 28 Absatz 2 lit. f u.E. fehlerhaft: Der englische Begriff „policies" sollte mit „Leitlinien" anstelle von „Richtlinien" übersetzt werden.

die bei Tests der (IKT-)Geschäftsfortführungspläne festgestellt werden (siehe Abschnitt 5.2);

- die nötigen Budgetmittel zuweist, um den Anforderungen an die digitale operationale Resilienz in Bezug auf alle Arten von Ressourcen gerecht zu werden; hiervon umfasst sind auch die IKT-Kompetenzen für alle Mitarbeiter. Dies sicherzustellen obliegt der Verantwortung des Leitungsorgans (Artikel 28 Absatz 2 lit. e und h RTS RMF) und ist mindestens jährlich zu überprüfen;

- die Modalitäten des Meldewesens an das Leitungsorgan über die Informationssicherheit und die digitale operationale Resilienz festlegt (Artikel 28 Absatz 2 lit. i RTS RMF); sowie

- den Bericht über die Überprüfung des vereinfachten IKT-Risikomanagementrahmens genehmigt und dies mit einem Datum versieht (Artikel 41 Absatz 2 lit. b RTS RMF).

Die in Kapitel 2.4/2.7 BAIT/VAIT vorgeschriebene Vermeidung von Interessenkonflikten durch geeignete organisatorische Maßnahmen ist auch im vereinfachten IKT-Risikomanagementrahmen Gegenstand der Anforderungen. Zwar ist die „Vermeidung von Interessenkonflikten" nicht explizit genannt, sie ergibt sich aber aus den Governance-Anforderungen und ist insbesondere hinsichtlich Kontrollfunktionen und internen Revisionsfunktionen in Artikel 28 Absatz 4 RTS RMF festgehalten. Die Aufgabe zur Festlegung von klaren Aufgaben und Verantwortlichkeiten für alle IKT-bezogenen Funktionen fällt gemäß Artikel 28 Absatz 2 lit. b RTS RMF dem Leitungsorgan zu.

Im vereinfachten IKT-Risikomanagementrahmen sind IKT-spezifische Anforderungen an die interne Revision aufgeführt: Der Rahmen soll im Einklang mit dem Revisionsplan des Finanzunternehmens einer internen Revision unterzogen werden. Dies umfasst auch die rechtzeitige Überprüfung und Auswertung kritischer Erkenntnisse der IKT-Revision (Artikel 28 Absatz 5 und 6 RTS RMF). Zudem müssen die Revisoren entsprechend über ausreichend Wissen und Kenntnisse im Bereich der IKT-Risiken verfügen.

3. Informationsrisiko- und Informationssicherheitsmanagement

In diesem Abschnitt werden die Vorgaben der Artikel 16 und 45 DORA und der Artikel 28-31 RTS RMF des vereinfachten IKT-Risikomanagementrahmens denen der Kapitel Informationsrisikomanagement und Informationssicherheitsmanagement der BAIT/VAIT (Kapitel 3 und 4 BAIT/VAIT) gegenübergestellt.

Der vereinfachte IKT-Risikomanagementrahmen führt angepasste und zum Teil neue Prüfungs- und Analyseanforderungen zu IKT-Risiken, Altsystemen, Vorfällen und Tests sowie damit verbundene Berichtspflichten ein, auch gegenüber der Aufsicht. So ist unter anderem eine regelmäßige oder anlassbezogene Überprüfung des vereinfachten IKT-Risikomanagementrahmens vorgesehen, die in Form eines Berichtes von der Aufsicht angefordert werden kann. Weiterhin betont DORA sowohl Schulungspflichten als auch Sensibilisierungsmaßnahmen vor dem Hintergrund der digitalen operationalen Resilienz.

3.1 Akzentverschiebung von Informationssicherheit zu IKT-Risikomanagement

Eine grundsätzliche Akzentverschiebung erfolgt durch die stärkere Betonung des IKT-Risikomanagements (Artikel 31 RTS RMF) gegenüber der Informationssicherheit. Im vereinfachten IKT-Risikomanagementrahmen ist das IKT-Risikomanagement die Grundlage zur Sicherstellung der digitalen operationalen Resilienz, wozu eine übergreifende Informationssicherheitsleitlinie und damit einhergehende IKT-Sicherheitsmaßnahmen zur Minderung des IKT-Risikos gefordert werden (Artikel 29 i.V.m. Artikel 30-38 RTS RMF); Informationssicherheitsrichtlinien zur Konkretisierung der Maßnahmen sind im Gegensatz zur BAIT/VAIT (Kapitel 4.3) nicht erforderlich.

Sowohl eine Genehmigung als auch eine Kommunikation dieser Leitlinie durch das Leitungsorgan ist nicht gefordert; die Festlegung der Ziele der Informationssicherheit sowie die Ermittlung, Bewertung und das Management der Informationssicherheitsleitlinie und der Maßnahmen fallen aber in den Aufgabenbereich des Leitungsorgans (Artikel 28 Absatz 1 lit. c und f RTS RMF, siehe Abschnitt 2.3). In den BAIT/VAIT liegt der Fokus hingegen auf den Informationssicherheitsmaßnahmen, die Risikobetrachtung folgt darauf. Eine stärkere Orientierung am IKT-Risiko auf Basis dieser Akzentverschiebung unter Einbezug bekannter Grundsätze und Regeln zum Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität von Daten und der von den Finanzunternehmen erbrachten Dienstleistungen, mit einer entsprechenden Priorisierung in der Umsetzung, ist aber durchaus denkbar.

Der Artikel 28 Absatz 3 RTS RMF weist explizit auf die Auslagerbarkeit der „Überprüfung der Einhaltung der Anforderungen für das IKT-Risikomanagement" hin, schränkt diese aber auf gruppeninterne IKT-Unternehmen oder IKT-Drittdienstleister ein. Im Falle einer Auslagerung[9] sind allerdings weiterhin sektorspezifische Anforderungen[10] an die Auslagerbarkeit zu beachten. Im konkreten Auslagerungsfall können diese sektoralen Regelungen durchaus Voraussetzungen, Bedingungen oder Grenzen für eine solche Auslagerung definieren. Auch bleibt das Finanzunternehmen für die Sicherstellung des IKT-Risikomanagements im vereinfachten Rahmen weiterhin uneingeschränkt verantwortlich.

Die Festlegung eines Informationsverbunds gemäß Kapitel 3.3/3.4 BAIT/VAIT und das Verfahren zur Schutzbedarfsfeststellung gemäß Kapitel 3.4/3.5 BAIT/VAIT werden durch die Klassifizierung von IKT- und Informationsassets (Artikel 3 Nr. 6 und 7 DORA) ersetzt (Artikel 28 Absatz 2 lit. d sublit. i, 30 Absatz 1 RTS RMF). Im vereinfachten IKT-Risikomanagementrahmen wird dabei auf die Ermittlung, Klassifizierung und Dokumentation von kritischen oder wichtigen Funktionen sowie auf IKT- und Informationsassets abgestellt, die diese Funktionen unterstützen (Artikel 30 Absatz 1 RTS RMF). Dabei sind wechselseitige Abhängigkeiten zu identifizieren sowie alle kritischen oder wichtigen Funktionen zu ermitteln, die von IKT-Drittdienstleistern unterstützt werden (Artikel 30 Absatz 2 RTS RMF). Bei der Klassifizierung der IKT-Assets besteht eine Verbindung zu dem gemäß Artikel 34 lit. a RTS RMF geforderten

[9] Ausgliederungen sind dabei miteingeschlossen.

[10] Beispielsweise Rundschreiben 06/2024 (BA) - Mindestanforderungen an das Risikomanagement (MaRisk), Rundschreiben 09/2025 (VA) - Aufsichtsrechtliche Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen unter Solvabilität II (MaGo für SII-VU) oder Leitlinien der Europäischen Aufsichtsbehörden zu Auslagerungen.

Lebenszyklusmanagement aller IKT-Assets, so dass eine Gesamtbetrachtung sinnvoll erscheint. Die Ermittlung und Klassifizierung ist bei Bedarf zu überprüfen (Artikel 30 Absatz 1 RTS RMF).

Durch die Verpflichtung, IKT- und Informationsassets und die Verbindungen/Interdependenzen zwischen den Assets zu erfassen, entsteht auch eine inhaltliche Nähe zu einer Configuration Management Database, deren Einsatz im vereinfachten IKT-Risikomanagementrahmen jedoch nicht gefordert wird. Wenn die Abdeckung der aufgeführten Besonderheiten sichergestellt ist, können die bekannten Verfahren zur Festlegung des Informationsverbunds i.V.m. der Anforderung zur Verwaltung von Komponenten der IT-Systeme aus dem IT-Betrieb und der Schutzbedarfsfeststellung zur Umsetzung herangezogen werden; andere Lösungsmöglichkeiten sind aber auch denkbar.

3.2 Fokus auf Bewertungs-, Analyse- und Kontrollhandlungen

Der in Kapitel 4.4/4.5 BAIT/VAIT vorgeschriebene Informationssicherheitsbeauftragte (ISB) findet keine Entsprechung im vereinfachten IKT-Risikomanagementrahmen. Auch eine IKT-Risikokontrollfunktion, wie sie der reguläre IKT-Risikomanagementrahmen gemäß Artikel 6 Absatz 4 DORA einführt, ist nicht vorgesehen.

Der vereinfachte IKT-Risikomanagementrahmen schreibt Prüfungs- und Analyse- sowie Bewertungsanforderungen zu IKT-Risiken, Altsystemen, Vorfällen und Tests sowie damit verbundene Berichtspflichten vor, teilweise auch gegenüber der Aufsicht. Dazu zählen insbesondere:

- Eine Dokumentation und Überprüfung des vereinfachten IKT-Risikomanagementrahmens gemäß Artikel 16 Absatz 2 DORA. Diese soll regelmäßig[11] oder anlassbezogen bei Auftreten schwerwiegender IKT-bezogener Vorfälle durchgeführt werden. Darauf baut eine kontinuierliche Verbesserung des vereinfachten IKT-Risikomanagementrahmens auf. Die Aufsicht kann einen Bericht zu der Überprüfung anfragen (Artikel 16 Absatz 2 DORA i.V.m. Artikel 41 RTS RMF). Die IKT-Risikobewertung hat unter Berücksichtigung des IKT-Risikoprofils des Finanzunternehmens regelmäßig zu erfolgen und ist zu dokumentieren (Artikel 31 Absatz 2 RTS RMF).

- Schlussfolgerungen aus der Analyse von IKT-bezogenen Vorfällen, größeren Veränderungen der IKT-Systeme oder IKT-Dienstleistungen sowie aus den Testergebnissen in Bezug auf die IKT-Sicherheit. Diese sind in den IKT-Risikoermittlungs- und -bewertungsprozess einzubeziehen (Artikel 16 Absatz 1 lit. h DORA i.V.m. Artikel 31 Absatz 1 lit. e RTS RMF).

- Die spezifischen Risiken für IKT-Altsysteme zu managen (Artikel 34 lit. e RTS RMF i.V.m. Artikel 3 DORA).

[11] Die Frequenz richtet sich gemäß Artikel 4 DORA i.V.m. Artikel 1 RTS RMF nach dem Grundsatz der Verhältnismäßigkeit, insbesondere nach der Größe, dem Gesamtrisikoprofil und der Komplexität des Geschäftsmodells des jeweiligen Finanzunternehmens.

Neben dem retrospektiven Blick auf IKT-bezogene Vorfälle sind für kritische oder wichtige Funktionen sowie für IKT- und Informationsassets relevante Bedrohungen und Schwachstellen fortlaufend zu überwachen (Artikel 31 Absatz 3 RTS RMF); Risikoszenarien, die sich auf kritische oder wichtige Funktionen auswirken, sind regelmäßig zu überprüfen.

3.3 Konkrete Anforderungen an Schulung und Kommunikation

Im vereinfachten IKT-Risikomanagementrahmen werden Schulungspflichten stärker als in den BAIT/VAIT betont. So haben Finanzunternehmen für ihre Mitarbeitenden und ihr Management Programme zur Sensibilisierung für IKT-Sicherheit und Schulungen zur digitalen operationalen Resilienz zu entwickeln (Artikel 16 Absatz 1 lit. h DORA i.V.m. Art 28 Absatz 2 lit. e RTS RMF). Wohingegen in den BAIT/VAIT ein kontinuierliches und angemessenes Sensibilisierungs- und Schulungsprogramm nur für Informationssicherheit festzulegen ist. Gegebenenfalls sind hier sektorale Governance-Anforderungen zu beachten.

Die in den BAIT/VAIT vorgesehene Kommunikation bzw. die Etablierung von Kommunikationswegen im Rahmen des Informationsrisiko- und Informationssicherheitsmanagements findet sich entsprechend im vereinfachten IKT-Risikomanagementrahmen nicht wieder. Generisch sieht der vereinfachte IKT-Risikomanagementrahmen allerdings die Etablierung eines IKT-spezifischen internen Governance- und Kontrollrahmens vor (siehe Abschnitt 2.2). Die Anforderungen an die (IKT-)Geschäftsfortführung gemäß Artikel 39 Absatz 2 lit. i RTS RMF konkretisieren allerdings Regelungen für die interne und externe Kommunikation (s. Abschnitt 5).

Sowohl die ausgeweiteten Anforderungen hinsichtlich der Fähigkeiten und Kenntnisse der Mitglieder des Leitungsorgans in Bezug auf IKT-Risiken (Artikel 5 Absatz 4 DORA) als auch an die Kommunikation, insbesondere zur verantwortungsbewussten Offenlegung von schwerwiegenden IKT-bezogenen Vorfällen oder Schwachstellen (Artikel 14 DORA) im regulären IKT-Risikomanagementrahmen, finden sich im vereinfachten Rahmen nicht wieder. Ungeachtet dessen müssen die Mitglieder des Leitungsorgans aufgrund ihrer Gesamtverantwortung hinsichtlich des vereinfachten IKT-Risikomanagementrahmens (Artikel 28 Absatz 2 lit. a RTS RMF), im Einklang mit den zu managenden IKT-Risiken, über angemessene IKT-Kompetenzen verfügen.

Finanzunternehmen können freiwillig an einem Informationsaustausch zu Cyberbedrohungen und -informationen innerhalb vertrauenswürdiger Gemeinschaften teilnehmen (Artikel 45 Absatz 1 DORA)[12]. Eine Teilnahme an einem solchen Informationsaustausch muss gegenüber der Aufsichtsbehörde gemeldet werden, ebenso ist die Beendigung der Zusammenarbeit mitzuteilen (Artikel 45 Absatz 3 DORA). Gemäß Artikel 49 Absatz 1 DORA können Aufsichtsbehörden Krisenmanagement- und Notfallübungen anbieten, um eine koordinierte Reaktion zu üben und Kommunikationskanäle zu entwickeln.

[12] Weitere Informationen finden Sie auf https://www.bafin.de/ref/19705730.

4. IT-Betrieb

In diesem Abschnitt werden die Vorgaben des Artikel 16 DORA sowie der Artikel 31, 34, 37, 38 und 39 RTS RMF im vereinfachten IKT-Risikomanagementrahmen an den Betrieb von IKT-Systemen dem Kapitel 8 IT-Betrieb der BAIT/VAIT gegenübergestellt.

Dem IT-Betrieb kommt im Rahmen der Stärkung der digitalen operationalen Resilienz eine hohe Bedeutung zu. Anforderungen an aktuelle, zuverlässige sowie technologisch resiliente IKT-Systeme sind auch im vereinfachten IKT-Risikomanagementrahmen enthalten. Die Klassifizierung der kritischen oder wichtigen Funktionen sowie der IKT- und Informationsassets, die diese Funktionen unterstützen, sorgen für ein ganzheitliches Bild der Systemlandschaft und Funktionen.

4.1 Betriebsstabilität mit vergleichbaren Anforderungen

Um die digitale operationale Resilienz zu stärken, liegt ein weiterer Schwerpunkt im vereinfachten IKT-Risikomanagementrahmen auf der Betriebsstabilität und der Aktualisierung von IKT-Systemen. Dies betont Artikel 16 Absatz 1 lit. b und c DORA und bildet damit vergleichbare Anforderungen zu den BAIT/VAIT ab. So fordert Artikel 16 Absatz 1 lit. c DORA „solide, resiliente und aktualisierte IKT-Systeme" – dies entspricht dem Umfang der bisherigen Anforderungen aus Kapitel 8.3 BAIT/VAIT.

Auch das aus Kapitel 8.8 BAIT/VAIT bekannte Kapazitätsmanagement wird durch Artikel 16 Absatz 1 lit. b DORA i.V.m. Artikel 34 lit. c RTS RMF aufgegriffen. Zur Verhinderung von IKT-Kapazitätsengpässen sind weiterhin Maßnahmen zum Kapazitätsmanagement notwendig. Dagegen sind die bisher in Kapitel 2.5/2.8 BAIT/VAIT adressierten angemessenen quantitativen oder qualitativen Kriterien (i.d.R. Kennzahlen) nicht mehr verpflichtend zur Steuerung des IT-Betriebs vorgesehen.

Darüber hinaus sind im vereinfachten IKT-Risikomanagementrahmen vergleichbare Anforderungen zu dem aus Kapitel 8.2/8.3 BAIT/VAIT bekannten Lebenszyklusmanagement enthalten. So sind gemäß Artikel 16 Absatz 1 lit. b und c DORA aktualisierte IKT-Systeme zu verwenden und deren Sicherheit fortlaufend zu überwachen. Im Vergleich zu Artikel 7 DORA des regulären IKT-Risikomanagementrahmens verweist der vereinfachte IKT-Risikomanagementrahmen nicht auf „stets auf dem neuesten Stand zu haltende IKT-Systeme, -Protokolle und –Tools".

Auch Risiken aus IKT-Altsystemen sind, wie auch in den BAIT/VAIT, gemäß Artikel 34 Absatz 1 lit. a und e RTS RMF zu managen. Allerdings ist eine jährliche Risikobewertung, die gemäß Artikel 8 Absatz 7 DORA im regulären IKT-Risikomanagementrahmen vorgesehen ist, nicht erforderlich.

4.2 Notwendige Klassifizierung der IKT- und Informationsassets

Wie in Abschnitt 3.1 beschrieben, sieht der vereinfachte IKT-Risikomanagementrahmen eine Klassifizierung der IKT- und Informationsassets vor. Im Fokus stehen dabei die Ermittlung, Klassifizierung und Dokumentation von kritischen oder wichtigen Funktionen sowie jener

IKT- und Informationsassets, die diese Funktionen unterstützen. Dabei sind auch die Wechselwirkungen der IKT-Assets untereinander zu berücksichtigen (Artikel 30 RTS RMF). Dieses Verfahren verbindet die bisherige getrennte Festlegung eines Informationsverbunds und die Auflistung der Komponenten der IT-Systeme (Kapitel 3 und 8 BAIT/VAIT) und erzeugt so ein ganzheitliches Bild über die IKT- und Informationsassets, welches bislang nicht in dieser Granularität gefordert war.

4.3 Verzicht auf Detailvorgaben bei Änderungen an IKT-Systemen

Der bereits aus Kapitel 8.4 und Kapitel 8.5 BAIT/VAIT bekannte risikoorientierte Ansatz des Änderungsmanagements wird im vereinfachten IKT-Risikomanagementrahmen in DORA weitergeführt (Artikel 37 und 38 RTS RMF), bringt aber Anpassungen mit sich: Die bisherige Betrachtung in den Rundschreiben der wesentlichen Änderungen wird durch eine Betrachtung aller Änderungen an IKT-Systemen im Rahmen des IKT-Änderungsmanagements abgelöst. Diese sind gemäß Artikel 38 Absatz 2 RTS RMF auf kontrollierte Weise zu erfassen, zu testen, zu bewerten, zu genehmigen, zu implementieren und zu überprüfen. Insgesamt ist zwar eine größere Menge an Änderungen als bisher zu betrachten, jedoch machen Artikel 37 und 38 RTS RMF weniger Detailvorgaben und enthalten weniger Mindestbestandteile als die BAIT/VAIT.

Weitere Informationen dazu folgen im Abschnitt 6.3 aus Sicht der Projektmanagements.

4.4 Wegfall des Datensicherungskonzepts

Kapitel 8.7 BAIT/VAIT fordert unter anderem eine Datensicherung und -wiederherstellung inklusive zugehöriger Tests. In Artikel 39 Absatz 2 lit. f und g RTS RMF werden diese Aspekte für den vereinfachten IKT-Risikomanagementrahmen zum Teil aufgegriffen.

Eine Datensicherung wird weiterhin verlangt. So bleiben Verfahren und Maßnahmen für die Datensicherung sowie Wiedergewinnungs- und Wiederherstellungsmaßnahmen für IKT-Assets bestehen. Auch ein regelmäßiges Testen dieser Anforderungen wird gemäß Artikel 40 RTS RMF weiterhin obligatorisch bleiben. Jedoch fordert der vereinfachte IKT-Risikomanagementrahmen kein Datensicherungskonzept mehr, da die technische Umsetzung im Vordergrund steht.

Die Meldung von ungeplanten Abweichungen vom Regelbetrieb (Störungen) aus Kapitel 8.6 BAIT/VAIT wird nicht mehr explizit gefordert. Der vereinfachte IKT-Risikomanagementrahmen verlangt gemäß Artikel 16 Absatz 1 lit. b RTS RMF eine fortlaufende Überwachung der Sicherheit und des Funktionierens der IKT-Systeme, setzt aber keine Mindestanforderungen an diese.

Die umfangreicheren Anforderungen des regulären IKT-Risikomanagementrahmens an die Richtlinie über Verfahren zum Backup sowie Verfahren und Methoden zur Wiedergewinnung und Wiederherstellung (Artikel 12 DORA) finden im vereinfachten IKT-Risikomanagementrahmen keine Anwendung.

Ferner verweist DORA auf umfangreiche Zusatzanforderungen zur Behandlung, Klassifizierung und Berichterstattung von IKT-bezogenen Vorfällen (vgl. Artikel 17-23 DORA) und das digitale operationale Testen (vgl. Artikel 24 und 25 DORA, Artikel 36 RTS RMF). Diese Artikel sind jedoch nicht Gegenstand der vorliegenden Umsetzungshinweise.

5. (IKT-)Geschäftsfortführung

In diesem Abschnitt werden die relevanten Vorgaben des Artikel 16 Absatz 1 lit. f und g DORA sowie der Artikel 39 und 40 RTS RMF für den vereinfachten IKT-Risikomanagementrahmen betreffend das Management der (IKT-)Geschäftsfortführung den Anforderungen zum (IT-)Notfallmanagement der BAIT/VAIT (jeweils Kapitel 10) gegenübergestellt.

Zusammenfassend ist festzuhalten, dass diese Anforderungen im vereinfachten IKT-Risikomanagementrahmen geringer ausfallen als die in Kapitel 10 BAIT/VAIT aufgeführten Anforderungen. Maßgebliche Unterschiede ergeben sich aus veränderten Inhalten und der Struktur der einschlägigen Pläne, Maßnahmen und Verfahren, in deren Mittelpunkt die (IKT-)Geschäftsfortführungspläne stehen.

Weitere Vereinfachungen im Vergleich zu den BAIT/VAIT ergeben sich bei der Überprüfung und dem Testen der (IKT-)Geschäftsfortführungspläne: Hier sieht der vereinfachte IKT-Risikomanagementrahmen regelmäßige Intervalle vor (zum Beispiel bei jeder größeren Veränderung der (IKT-)Geschäftsfortführungspläne) beziehungsweise in Bezug auf Sicherungs- und Wiedergewinnungsverfahren mindestens jährliche Intervalle und harmonisiert damit die Anforderungen der BAIT/VAIT. Überdies sind, wie auch in den VAIT im Rahmen des (IT-)Notfallkonzepts, Regelungen zur Kommunikation als Bestandteil der (IKT-)Geschäftsfortführungspläne vorgesehen.

Insgesamt ist auch hier zu beachten, dass Anforderungen zu der Geschäftsfortführung beziehungsweise zu dem Notfallmanagement aus sektoralen Vorschriften weiter Anwendung finden und DORA diese in Bezug auf ihre Regelungen zur digitalen operationalen Resilienz insoweit ergänzt.

Im Vergleich zum regulären IKT-Risikomanagementrahmen ist im vereinfachten IKT-Risikomanagementrahmen keine Meldung an die zuständigen Behörden über die geschätzten aggregierten jährlichen Kosten und Verluste vorgesehen, die durch schwerwiegende IKT-bezogene Vorfälle verursacht wurden (vgl. Artikel 11 Absatz 10 DORA).

5.1 Veränderte und vereinfachte Struktur und Inhalte

Zentrale Elemente in der (IKT-)Geschäftsfortführung sind im vereinfachten IKT-Risikomanagementrahmen gemäß Artikel 16 Ab. 1 lit. f DORA die (IKT-)Geschäftsfortführungspläne sowie Gegen- und Wiederherstellungsmaßnahmen, die zumindest Sicherungs- und Wiedergewinnungsmaßnahmen umfassen. Diese fußen, wie auch in den BAIT/VAIT vorgesehen, auf Klassifizierungsanforderungen, der Business-Impact-Analyse und einer Risikoanalyse (Artikel 28 Absatz 2 lit. d i.V.m. Artikel 30 und 39 Absatz 1 RTS RMF).

Der vereinfachte IKT-Risikomanagementrahmen fordert keine Zielfestlegung im Rahmen eines Notfall- (BAIT) bzw. IT-Notfallmanagements (VAIT). Die Ziele werden dagegen im vereinfachten IKT-Risikomanagementrahmen in den (IKT-)Geschäftsfortführungsplänen festgelegt, die auch in den BAIT/VAIT vorgesehen sind (vgl. Kapitel 8.7, 10.1 BAIT und 8.7 VAIT). Damit soll die Kontinuität kritischer oder wichtiger Funktionen sichergestellt werden.

Ebenso enthält der vereinfachte Rahmen kein (IT-)Notfallkonzept mit seinen IT-Notfallplänen, die Wiederanlauf-, Notbetriebs- und Wiederherstellungspläne umfassen (vgl. insbesondere Kapitel 10.3/10.5 BAIT/VAIT). Stattdessen sind in diesem Kontext Gegen-, Wiedergewinnungs- und Wiederherstellungsmaßnahmen vorgesehen
(Artikel 16 Absatz 2 lit. f DORA und Artikel 39 Absatz 2 lit. f RTS RMF).

Folgende Anforderungen und Komponenten an die (IKT-)Geschäftsfortführung sind gemäß Artikel 39 Absatz 2 RTS RMF in den (IKT-)Geschäftsfortführungsplänen zu spezifizieren:

- Genehmigung durch das Leitungsorgan (i.V.m. Artikel 28 Absatz 2 lit. d sublit. ii RTS RMF, siehe Abschnitt 2.3). In den VAIT hingegen verantwortete die Geschäftsleitung die Erstellung eines IT-Notfallkonzepts im Rahmen des IT-Notfallmanagements (Kapital 10.2 VAIT).

- Dokumentation und leichte Zugänglichkeit im Not- oder Krisenfall. In den VAIT war dies in Bezug auf die IT-Notfallpläne gefordert.

- Ausreichende Mittel für die Ausführung (i.V.m. Artikel 28 Absatz 2 lit. e RTS RMF, siehe Abschnitt 2.3). In den BAIT/VAIT ist dies allgemein in Bezug auf die quantitativ und qualitativ angemessene Personal- bzw. Ressourcenausstattung aufgeführt (Kapitel 2.1 BAIT/VAIT) aber nicht spezifisch für das (IT-)Notfallmanagement.

- Nennung der geplanten Wiederherstellungsniveaus und der Zeitrahmen für die Wiederherstellung und Wiederaufnahme von Funktionen sowie Ermittlung der Wiedergewinnungs- und Wiederherstellungsmaßnahmen für kritische oder wichtige Geschäftsfunktionen, unterstützende Prozesse, IKT- und Informationsassets (siehe Abschnitt 4.4) sowie deren Interdependenzen. Hierzu gehören auch Maßnahmen zur Minderung von Ausfällen von IKT-Drittdienstleistern. In den BAIT/VAIT finden sich vergleichbare Anforderungen in Kapitel 10.3/10.5 BAIT/VAIT im Rahmen der Parameter für die IT-Notfallpläne wieder.

- Festlegung der Bedingungen zur Aktivierung der (IKT-)Geschäftsfortführungspläne und der zu ergreifenden Maßnahmen, um die Verfügbarkeit, Kontinuität und Wiederherstellung der IKT-Assets der Finanzunternehmen zur Unterstützung kritischer oder wichtiger Funktionen sicherzustellen. In den VAIT war die Aktivierung der IT-Notfallpläne in Kapitel 10.5 aufgeführt.

- Erwägung von Alternativen für den Fall, dass eine Wiederherstellung wegen Kosten, Risiken, Logistik oder unvorhergesehener Umstände kurzfristig nicht durchführbar sein könnte. In den VAIT waren derartige Alternativen im Rahmen der Parameter für die IT-Notfallpläne zu berücksichtigen (Kapitel 10.5 VAIT).

- Festlegung von Regelungen für die interne und externe Kommunikation, insbesondere durch Eskalationspläne (siehe Abschnitt 5.3).

Die (IKT-)Geschäftsfortführungspläne sind zu aktualisieren, um den Lehren aus Vorfällen, Tests, neuen Risiken und ermittelten Bedrohungen, veränderten Wiederherstellungszielen sowie größeren Veränderungen der Organisation des Finanzunternehmens und der IKT-Assets zur Unterstützung kritischer oder geschäftlicher Funktionen Rechnung zu tragen (Artikel 39 Absatz 2 lit. j RTS RMF). Die Aktualisierung soll in einem angemessenen Verhältnis zum (IKT-)Risikoprofil des Finanzunternehmens stehen. Gemäß Kapitel 10.5 VAIT waren sowohl das IT-Notfallkonzept als auch die IT-Notfallpläne anlassbezogen zu aktualisieren sowie regelmäßig auf Aktualität zu überprüfen; die BAIT sehen in Kapitel 10.4 bei zeitkritischen Aktivitäten und Prozessen eine Überprüfung für alle relevanten Szenarien mindestens jährlich und anlassbezogen vor.

Wie in Abschnitt 3.2 erörtert, ist der vereinfachte IKT-Risikomanagementrahmen, zu dem die (IKT-)Geschäftsfortführung gehört, regelmäßig[13] und bei Auftreten schwerwiegender IKT-bezogener Vorfälle entsprechend den aufsichtlichen Anweisungen zu überwachen, zu überprüfen und zu dokumentieren.

Auch im Vergleich zu dem regulären IKT-Risikomanagementrahmen finden sich Vereinfachungen: Sowohl die vorgesehene IKT-Geschäftsfortführungsleitlinie (Artikel 11 Absatz 1 DORA) als auch die IKT-Reaktions- und Wiederherstellungspläne (Artikel 11 Absatz 3 DORA) sind nicht Gegenstand der Anforderungen im vereinfachten IKT-Risikomanagementrahmen.

5.2 Notwendigkeit des Testens und der Verwendung von Szenarien

Wie auch in den BAIT/VAIT ist das Testen ein essentieller Bestandteil der Anforderungen an die (IKT-)Geschäftsfortführung im vereinfachten IKT-Risikomanagementrahmen und soll nachweisen, dass die Pläne und Verfahren ihren Zweck erfüllen sowie etwaige Mängel aufdecken (Artikel 40 Absatz 2 RTS RMF). Hier sind die (IKT-)Geschäftsfortführungspläne, insbesondere auch hinsichtlich der in ihnen genannten Szenarien, zu testen (Artikel 40 RTS RMF).

Das Testen hat hinsichtlich der Sicherungs- und Wiedergewinnungsverfahren mindestens jährlich und bei jeder größeren Veränderung der Pläne zu erfolgen (Artikel 40 Absatz 1 RTS RMF). Getestet werden auch die in den (IKT-)Geschäftsfortführungsplänen genannten Szenarien. Diese sind aber, anders als in den BAIT/VAIT, nur für einen Cyberangriff und der Berücksichtigung von schwerwiegenden Betriebsstörungen weiter spezifiziert (Artikel 39 Absatz 1 RTS RMF). Die Erstellung eines (IT-)Testkonzepts, mit denen IT-Notfallpläne regelmäßig (VAIT) bzw. mindestens jährlich (BAIT) und anlassbezogen zu testen sind, ist nicht Gegenstand der Anforderungen des vereinfachten IKT-Risikomanagementrahmens.

[13] Die Frequenz richtet sich gemäß Artikel 4 DORA i.V.m. Artikel 1 RTS RMF nach dem Grundsatz der Verhältnismäßigkeit, insbesondere nach der Größe, dem Gesamtrisikoprofil und der Komplexität des Geschäftsmodells des jeweiligen Finanzunternehmens.

Die Ergebnisse der Tests der (IKT-)Geschäftsfortführungspläne sind zu dokumentieren und etwaige bei diesen Tests festgestellte Mängel müssen analysiert, behoben und dem Leitungsorgan gemeldet werden (Artikel 40 Absatz 3 RTS RMF, siehe Abschnitt 2.3).

Im Vergleich zum regulären IKT-Risikomanagementrahmen zeigen sich Vereinfachungen unter anderem bei den zu verwendenden Szenarien (vgl. Artikel 26 Absatz 2 RTS RMF): Deren Zahl fällt im vereinfachten IKT-Risikomanagementrahmen deutlich geringer aus.

5.3 Kommunikation als Gegenstand der (IKT-)Geschäftsfortführungspläne

Regelungen zur internen und externen Kommunikation sind im vereinfachten IKT-Risikomanagementrahmen Gegenstand der (IKT-)Geschäftsfortführungspläne (Artikel 39 Absatz 2 lit. i RTS RMF). Dazu gehören insbesondere auch Eskalationspläne, die nicht in den BAIT/VAIT genannt sind. In den VAIT war eine angemessene Kommunikation des IT-Notfallkonzepts und der IT-Notfallpläne vorgesehen (Kapitel 10.2 und 10.5 VAIT).

Im Gegensatz zum regulären IKT-Risikomanagementrahmen sieht der vereinfachte Rahmen keine Krisenmanagementfunktion vor (Artikel 11 Absatz 7 DORA).

6. IT-Projektmanagement und Anwendungsentwicklung

In diesem Abschnitt werden die Vorgaben der Artikel 37 und 38 RTS RMF an das IKT-Projekt- und Änderungsmanagement im vereinfachten IKT-Risikomanagementrahmen den Anforderungen an das IT-Projektmanagement und die Anwendungsentwicklung der Kapitel 7 BAIT/VAIT gegenübergestellt.

Insgesamt ist festzuhalten, dass die Einzelanforderungen mit spezifischer IKT-Sicherheitsausprägung im vereinfachten IKT-Risikomanagementrahmen deutlich weniger Details enthalten, als die BAIT/VAIT im Kapitel zu IT-Projekten und Anwendungsentwicklung. Der Fokus im vereinfachten Rahmen liegt klar auf der Implementierung von geeigneten Maßnahmen zur Erfüllung der Sicherheitsziele und weniger auf der Governance von bestimmten Prozessen, wie in den BAIT/VAIT. Die Anforderungen in DORA stellen Mindestanforderungen dar und sollten nicht als abschließend interpretiert werden. Flankierende Maßnahmen zu diesen Mindestanforderungen können auch hier nach dem Grundsatz der Verhältnismäßigkeit eingefordert werden.

Im Vergleich zum regulären IKT-Risikomanagementrahmen sind die Anforderungen im vereinfachten IKT-Risikomanagementrahmen weniger detailliert.

6.1 Allgemeine Anforderungen im IKT-Projektmanagement

Auch im vereinfachten IKT-Risikomanagementrahmen sind, analog zu den Kapiteln 7.3/7.4 BAIT/VAIT, die grundsätzlichen Anforderungen an eine IKT-Projektmethodik enthalten, die in einem entsprechenden Verfahren umzusetzen sind (Artikel 38 Absatz 1 RTS RMF). Erleichterungen ergeben sich bei der Betrachtung von Korrelationen über mehrere Projekte hinweg. Hier sehen die BAIT/VAIT vor, dass eine

Risikobetrachtung bezüglich der Abhängigkeiten von IT-Projekten untereinander zu erfolgen hat. Der vereinfachte IKT-Risikomanagementrahmen fordert diese Betrachtung nicht mehr.

Explizite Anforderungen bzgl. einer Projektdokumentation und Lessons-Learned sind nicht Bestandteil des vereinfachten IKT-Risikomanagementrahmens. Dieser fordert lediglich, dass das IKT-Projektmanagementverfahren alle Projektphasen abbildet und klare Zuständigkeiten definiert.

6.2 Keine Detailvorgaben zu IKT-System Beschaffung, Entwicklung und Wartung

Im Vergleich zu den BAIT/VAIT sind die Anforderungen des vereinfachten IKT-Risikomanagementrahmens deutlich weniger detailliert und enthalten wenige Mindestbestandteile für ein risikobasiertes Verfahren zur Beschaffung, Entwicklung und Wartung (Artikel 37 RTS RMF). Im Gegensatz zu den BAIT/VAIT liegt der Fokus weniger auf der Dokumentation der Anwendungsentwicklung und stattdessen mehr auf der Vorgabe der zur Umsetzung benötigten Anforderungen (Artikel 37 lit. a RTS RMF), des Testens (Artikel 37 lit. b RTS RMF) und der sicheren Implementierung (Artikel 37 lit. c RTS RMF). Eine vollständige Dokumentation von Anforderungen im Sinne eines Fachkonzepts oder Lastenhefts wird nicht explizit gefordert.

Beispielsweise verlangt Artikel 37 lit. a RTS RMF, dass die (nicht)funktionalen Anforderungen (inklusive Informationssicherheit) vor Beschaffung oder Entwicklung der IKT-Systeme von der betreffenden Unternehmensfunktion klar spezifiziert und genehmigt werden.

Gemäß Artikel 37 lit. b RTS RMF sind IKT-Systeme vor ihrer Einführung bzw. vor Einführung von Änderungen an der Produktionsumgebung zu testen und zu genehmigen. Die VAIT forderten an dieser Stelle hingegen lediglich die Einführung eines Regelprozesses, ohne konkrete Testverfahren oder Szenarien zu benennen.

Im Vergleich zu den BAIT/VAIT werden im vereinfachten IKT-Risikomanagementrahmen keine Anforderungen an Stressbelastungsszenarien gestellt.

Im Umgang mit Quellcode aus der Anwendungsentwicklung enthält der vereinfachte IKT-Risikomanagementrahmen keine expliziten Anforderungen. Die Anforderungen an die Integrität von Anwendungen sind daher mit den BAIT/VAIT vergleichbar.

Explizite Anforderungen an die individuelle Datenverarbeitung (IDV) sind im vereinfachten IKT-Risikomanagementrahmen nicht enthalten. So wird keine Unterscheidung zwischen IDV und zugekauften (Standard-)Anwendungen getroffen.

6.3 Wegfall der Wesentlichkeitsgrenze im IKT-Änderungsmanagement

Kapitel 7.1 BAIT/VAIT sieht vor, dass wesentliche Änderungen der IT-Systeme einem vorgeschriebenen Analyseprozess unterliegen müssen und in Abhängigkeit zur Wesentlichkeit der Änderungen weitere, betroffene Organisationseinheiten zu beteiligen sind. Der vereinfachte IKT-Risikomanagementrahmen unterscheidet nicht mehr zwischen

wesentlicher und nicht wesentlicher Änderung. Daher müssen Finanzunternehmen ein Verfahren umsetzen um sicherzustellen, dass künftig alle Änderungen an IKT-Systemen auf kontrollierte Weise und mit angemessenen Schutzvorkehrungen aufgezeichnet, getestet, bewertet, genehmigt, implementiert und verifiziert werden (Artikel 38 Absatz 2 RTS RMF).

Die in den BAIT/VAIT vorgesehene Beteiligung weiterer Organisationseinheiten wird im vereinfachten IKT-Risikomanagementrahmen nicht explizit gefordert.

7. IKT-Drittparteienrisikomanagement

In diesem Abschnitt werden für Finanzunternehmen, die unter den vereinfachten IKT-Risikomanagementrahmen (Artikel 16 DORA) fallen, die Anforderungen der Artikel 28-30 DORA und des RTS SUB an das IKT-Drittparteienrisikomanagement denen des Kapitels 9 der BAIT („Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen") bzw. des Kapitels 9 der VAIT („Ausgliederungen von IT-Dienstleistungen und sonstige Dienstleistungsbeziehungen im Bereich IT-Dienstleistungen") gegenübergestellt.[14] Auszüge der Mindestanforderungen an das Risikomanagement (AT 9 MaRisk) sowie der Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen unter Solvabilität II beziehungsweise von Einrichtungen der betrieblicher Altersversorung (Kapitel 13 MaGo für S II-VU bzw. Kapitel 12 MaGo für EbAV)[15] werden aufgrund der engen Verflechtung mit den Anforderungen der BAIT/VAIT ebenfalls betrachtet.

DORA regelt in den genannten Artikeln die Nutzung von IKT-Dienstleistungen, die von IKT-Drittdienstleistern bereitgestellt werden, welche bis auf wenige Ausnahmen auch im vereinfachten IKT-Risikomanagementrahmen gelten. Dazu werden eine Reihe von Schlüsselprinzipien für ein solides Management des IKT-Drittparteienrisikos definiert. Diese umfassen Anforderungen an die Governance, den Lebenszyklus eines IKT-Dienstleistungsbezugs, den Umgang mit bestimmten IKT-Drittparteienrisiken und die Mindestvertragsinhalte. Eine Auflistung der Mindestvertragsinhalte ist auf der Webseite der BaFin veröffentlicht.

7.1 Abgrenzung zu Auslagerung und Ausgliederung

Das IKT-Drittparteienrisikomanagement nach DORA ergänzt die bestehenden sektoralen Regelungen zu Auslagerungen oder Ausgliederungen[16] (im Folgenden nur „Auslagerung"). Die sektorspezifischen Auslagerungsanforderungen sind somit weiterhin zu beachten, d. h., sowohl die gesetzlichen Anforderungen als auch die Vorgaben zum Beispiel aus den MaRisk oder MaGo sind weiterhin anwendbar, sie bestehen parallel und komplementär. Dadurch ist

[14] Eine vollständige Darstellung des IKT-Drittparteienrisikomanagements nach DORA kann dem Abschnitt 6 der im Juni 2024 veröffentlichten Aufsichtsmitteilung „Hinweise zur Umsetzung von DORA im IKT-Risikomanagement und IKT-Drittparteienrisikomanagement" entnommen werden.

[15] Im Folgenden sind mit dem Begriff MaGo immer MaGo für SII-VU und MaGo für EbAV gemeint, sofern nicht explizit anders dargestellt.

[16] DORA Erwägungsgrund 29: „Daher müssen bestimmte Schlüsselprinzipien festgelegt werden, die Finanzunternehmen als Richtschnur für das Management des IKT-Drittparteienrisikos dienen […]. Diese Prinzipien ergänzen die für die Auslagerung geltenden sektorspezifischen Rechtsvorschriften."

anzunehmen, dass in vielen Fällen eine vertragliche Vereinbarung über die Nutzung von IKT-Dienstleistungen auch eine Auslagerung darstellt (und umgekehrt). Eine Harmonisierung der Anforderungen an das IKT-Drittparteienrisikomanagement unter DORA und der sektoralen Anforderungen an Auslagerungen wird aufsichtsseitig angestrebt.

Aus diesem Grund betrachtet dieser Abschnitt nicht allein die wesentlichen Auswirkungen aus Unterschieden zwischen DORA und BAIT/VAIT, sondern auch die einschlägigen Abschnitte der MaRisk und MaGo.

Die Definition von vertraglichen Vereinbarungen zur Nutzung von IKT-Dienstleistungen (Artikel 28 Absatz 1 lit. a i.V.m. Artikel 3 Nr. 21 DORA) ist deutlich weiter gefasst, als die bisherigen Auslagerungsdefinitionen, insbesondere, weil sie sich für Finanzunternehmen auf alle „IKT-Dienstleistungen für die Ausübung ihrer Geschäftstätigkeit" bezieht. Dadurch wird eine Einwertung aller Drittbezüge mit IKT-Bezug notwendig und es ergeben sich in der Umsetzung ggf. Unsicherheiten zur korrekten Klassifizierung. Zusätzlich ist in vielen Fällen mit einer Ausweitung der abzudeckenden Sachverhalte zu rechnen.

Von besonderer Bedeutung für den Umfang der zu erfüllenden Anforderungen ist, ob die bezogene IKT-Dienstleistung eine kritische oder wichtige Funktion unterstützt. In einem solchen Fall wird von einer besonderen Bedeutung der verbundenen IKT-Drittparteienrisiken ausgegangen. Die Bewertung von Funktionen als „kritisch oder wichtig" ist methodisch und inhaltlich nicht identisch mit einer Wesentlichkeitsbestimmung bei Auslagerungen.[17] Sie erfolgt auf Basis der Auswirkungen, die ein Ausfall oder eine eingeschränkte Leistung der Funktion zur Folge hätte (Artikel 3 Nr. 22 DORA). Auch hier ist die Entwicklung von geeigneten Kriterien zur Einstufung und die Bewertung aller Sachverhalte notwendig.

7.2 Allgemeine Erleichterungen

Im vereinfachten IKT-Risikomanagementrahmen gelten im Grundsatz alle Anforderungen der Artikel 28-30 DORA. Es bestehen aber Erleichterungen, die im Wesentlichen folgende Punkte umfassen:

- Die umfassenden Anforderungen an die Governance des IKT-Drittparteienrisiko-managements aus den Artikeln 5 und 6 DORA des regulären IKT-Risikomanagementrahmens sind nicht anwendbar. Dies bedeutet insbesondere, dass Finanzunternehmen, die den vereinfachten IKT-Risikomanagementrahmen anwenden, gemäß Artikel 28 Absatz 2 DORA keine IKT-Drittparteienrisikostrategie verabschieden müssen. In der Folge müssen sie auch keine Leitlinie für die Nutzung von IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen, erstellen, da diese Leitlinie ein Teil der IKT-Drittparteienrisikostrategie ist. Der mit dieser Leitlinie verbundene RTS-TPPol[18] muss somit ebenfalls nicht berücksichtigt werden.

[17] Bzw. Bewertung der Frage, ob eine wichtige Funktion oder Versicherungstätigkeit/Versorgungstätigkeit i. S. d. VAG vorliegt.

[18] Delegierte Verordnung (EU) 2024/1773 der Kommission vom 13. März 2024 zur Ergänzung der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Spezifizierung des detaillierten Inhalts der Leitlinie für vertragliche Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen, die von IKT-Drittdienstleistern bereitgestellt werden

- Bei der Betrachtung der Abhängigkeiten von IKT-Drittdienstleistern wird im vereinfachten IKT-Risikomanagementrahmen nach Artikel 16 Absatz 1 lit. e DORA nur die Ermittlung von wesentlichen Abhängigkeiten gefordert, dazu gehören solche, die kritische oder wichtige Funktionen unterstützen (Artikel 30 Absatz 2 RTS RMF, zum Begriff siehe Abschnitt 7.1).

- Eine Berichterstattung zum IKT-Drittparteienrisikomanagement mit festgelegten Berichtsintervallen (zum Beispiel quartärlich) oder formalisierte Meldekanäle, wie sie in den sektoralen Auslagerungsanforderungen gefordert wurden, sind nicht mehr vorgeschrieben, so dass mehr Flexibilität bei der Ausgestaltung besteht.

- Im Gegensatz zu den MaRisk/MaGo muss auch keine mit dem Zentralen Auslagerungsbeauftragten oder Ausgliederungsbeauftragten vergleichbare Funktion eingerichtet werden, so dass auch bei der organisatorischen Gestaltung der Überwachung von Auslagerungen mehr Gestaltungsspielräume bestehen (siehe aber Abschnitt 7.1).

7.3 Ausweitung der Vertragsanforderungen

Mit DORA geht im Vergleich zu den MaRisk oder anderen sektoralen Vorschriften eine deutliche Ausweitung der mit dem IKT-Drittdienstleister verpflichtend zu vereinbarenden Vertragsinhalte[19] einher. Diese sind insbesondere:

- Formvorschriften, unter anderem Form und Abbildung in einem Dokument (Artikel 30 Absatz 1 DORA),

- Mindestinhalte für alle vertraglichen Vereinbarungen (Artikel 30 Absatz 2 DORA),

- Zusätzliche Mindestinhalte für vertragliche Vereinbarungen zur Unterstützung kritischer oder wichtiger Funktionen (Artikel 30 Absatz 3 DORA),

- Kündigungsrechte (Artikel 28 Absatz 7 DORA sowie Artikel 6 RTS SUB),

- Prüfrechte (Artikel 30 Absatz 3 lit. e DORA und Artikel 4 Absatz 1 lit. j RTS SUB),

- Verpflichtung der Nachbildung der relevanten Vertragsinhalte bei Unterauftragsvergaben zur Unterstützung kritischer oder wichtiger Funktionen (Artikel 3 Absatz 1 lit. c RTS SUB),

- Beschreibung und Bedingungen, unter denen eine Unterauftragsvergabe zulässig ist (Artikel 30 Absatz 2 lit. a DORA und Artikel 4 RTS SUB), sowie

- eine ausreichende Mitteilungsfrist im Fall von wesentlichen Veränderungen bei Unterauftragsvergaben für kritische oder wichtige Funktionen und Verpflichtung, in dieser Frist keine Änderungen zu vollziehen, sowie das Recht, Änderungen zu verlangen (Artikel 5 RTS SUB).

[19] In die Auflistung wurden nur Anforderungen aufgenommen, die auf Level 1 oder Level 2 explizit als Mindestvertragsinhalte dargestellt sind. Weitere Vertragsinhalte, die sich aus anderen Anforderungen ergeben, oder die sinnvollerweise vereinbart werden sollten, wurden nicht aufgenommen.

Durch die deutliche Ausweitung des Anwendungsbereichs und der verpflichtend zu vereinbarenden Vertragsinhalte ist in vielen Fällen eine Neu- bzw. Nachverhandlung eines großen Teils der Verträge mit IKT-Drittdienstleistern notwendig. Hinzu kommt, dass die verpflichtenden Vertragsinhalte auch vertragliche Vereinbarungen abdecken, die nicht kritische oder wichtige Funktionen unterstützen bzw. keine wesentlichen Auslagerungen[20] betreffen.

Es sollen bei Vertragsabschluss Standardvertragsklauseln berücksichtigt werden, die von Behörden für bestimmte Dienstleistungen entwickelt wurden (Artikel 30 Absatz 4 DORA). Standardvertragsklauseln können von den zuständigen europäischen Behörden veröffentlicht werden. Aktuell liegen allerdings keine Standardvertragsklauseln vor, Finanzunternehmen sollten daher nicht die Veröffentlichung von Standardvertragsklauseln zur Umsetzung der Mindestvertragsinhalte abwarten.

Es sind keine erweiterten Übergangsfristen für die Anpassung der bestehenden vertraglichen Vereinbarungen (Risikoanalysen, Vertragsinhalte) vorgesehen. Die Anpassung der vertraglichen Vereinbarungen soll sobald wie möglich vorgenommen werden.

7.4 Neuregelung von Unterauftragsvergaben

Unterauftragsvergaben für kritische oder wichtige Funktionen werden in dem RTS SUB umfassend geregelt. In dem RTS kommt es zu einer deutlichen Ausweitung der Regulierungsbreite und -tiefe:

- Feststellung des Vorliegens der Bedingungen für die Unterauftragsvergabe durch das Finanzunternehmen (Artikel 4 RTS SUB): der IKT-Drittdienstleister muss unter anderem dazu in der Lage sein, einen geeigneten Unterauftragnehmer auszuwählen und angemessen zu überwachen (Artikel 3 Absatz 1 lit. a und e RTS SUB),
- Vertragsinhalte bezogen auf Unterauftragnehmer (Artikel 4 RTS SUB) und
- Vorgehen bei wesentlichen Änderungen (Artikel 5 RTS SUB) und ggf. damit verbundene Kündigungsrechte (Artikel 6 RTS SUB).

7.5 Umfangreiche Anforderungen an Risikobewertungen und Due-Diligence

Der Umfang der Anforderungen an Risikobewertungen und Due-Diligence, insbesondere bei vertraglichen Vereinbarungen, die kritische oder wichtige Funktionen betreffen, sind im Vergleich zu den sektoralen Auslagerungsanforderungen gestiegen. Dies betrifft vor allem den Inhalt und die Tiefe der Analyse. Die Inhalte für IKT-Dienstleistungen, die keine kritischen oder wichtigen Funktionen unterstützen, werden nur recht allgemein ausgeführt:

- Beurteilung der Einhaltung aufsichtsrechtlicher Bedingungen (Artikel 28 Absatz 4 lit. b DORA),

[20] Für kleine EbAV und Versicherungsholdings im Sinne des § 7 Nr. 31 VAG und im Sinne des § 293 Absatz 4 VAG die Bewertung, ob eine wichtige Funktion oder Versicherungstätigkeit/Versorgungstätigkeit i. S. d. VAG vorliegt.

- Ermittlung und Bewertung aller relevanten Risiken, einschließlich des IKT-Konzentrationsrisikos (Artikel 28 Absatz 4 lit. c DORA),

- Eignung des IKT-Drittdienstleisters im Rahmen einer Due-Diligence (Artikel 28 Absatz 4 lit. d DORA),

- Ermittlung und Bewertung von Interessenkonflikten (Artikel 28 Absatz 4 lit. e DORA) sowie die

- Einhaltung angemessener Standards der Informationssicherheit (Artikel 28 Absatz 5 DORA).

Bei IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen, kommen weitere zu analysierende Sachverhalte hinzu, die im Umfang die bisherigen Anforderungen zum Teil deutlich übersteigen:

- Abwägung der Vorteile und Risiken im Zusammenhang mit Unterauftragsvergaben (Artikel 29 Absatz 2 DORA, Artikel 1 RTS SUB) und Bewertung langer und komplexer Ketten der Unterauftragsvergabe (Artikel 29 Absatz 2 DORA);

- Berücksichtigung von Rechtsrisiken, d. h. der Bestimmungen des Insolvenzrechts (Artikel 29 Absatz 2 DORA) und bei Drittländern die Einhaltung und Durchsetzbarkeit von Rechtsvorschriften und die Einhaltung von Datenschutzvorschriften (Artikel 29 Absatz 2 DORA); und

- Angemessene Berücksichtigung von „aktuellsten und höchsten Qualitätsstandards für die Informationssicherheit“ (Artikel 28 Absatz 5 DORA).

7.6 Geänderte Anforderungen an den Ausstieg

Die Anforderungen an Ausstiegsstrategien/-pläne für IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen steigen im Vergleich zu den sektoralen Auslagerungsanforderungen deutlich, insbesondere sind die Erwartungen an die Ziele der Ausstiegsstrategien deutlich ausgeweitet (Artikel 28 Absatz 8 DORA). So sollen Finanzunternehmen ohne Unterbrechung ihrer Geschäftstätigkeit und ohne Beeinträchtigung ihrer für Kundinnen und Kunden erbrachten Dienstleistungen oder der Einhaltung regulatorischer Anforderungen aus vertraglichen Vereinbarungen ausscheiden können. Die Ausstiegspläne sind ausreichend zu testen und sollen regelmäßig[21] überprüft werden.

Die bisherige Öffnungsklausel für gruppen- oder verbundinterne Auslagerungen bei Kreditinstituten (Verzicht auf Ausstiegsprozesse gemäß AT 9 Tz. 15 MaRisk) entfällt, wenn diese gleichzeitig IKT-Dienstleistungen sind. Eine Berücksichtigung der Verhältnismäßigkeit ist aber weiterhin in Bezug auf ein reduziertes Risiko (insoweit zutreffend) möglich. Dies betrifft auch IKT-Drittdienstleister, die selbst unter Aufsicht stehen oder überwacht werden, es sei denn die

[21] Die Frequenz richtet sich gemäß Artikel 4 Absatz 2 i.V.m. Artikel 28 Absatz 1 lit. b DORA nach dem Grundsatz der Verhältnismäßigkeit.

erbrachte Dienstleistung ist als regulierte Finanzdienstleistung nicht als IKT-Dienstleistung nach DORA einzustufen.[22]

Unter DORA kommt es zu einer umfangreichen und sehr konkreten Berücksichtigung von Konzentrationsrisiken mit dem Ziel, diese zu ermitteln und angemessen zu überwachen. Dazu wird bei vertraglichen Vereinbarungen, die kritische oder wichtige Funktionen betreffen, ermittelt und bewertet, ob der IKT-Drittdienstleister nicht ohne Weiteres ersetzbar wäre oder ob es einen mehrfachen Bezug von IKT-Dienstleistungen von einem IKT-Drittdienstleister gibt. Wenn Konzentrationsrisiken vorliegen, müssen Finanzunternehmen den Nutzen und die Kosten alternativer Lösungen abwägen (Artikel 29 Absatz 1 DORA). Dieses Konzentrationsrisiko fließt sowohl in die ex-ante Risikobewertung ein als auch in die Analysen für Unterauftragsvergaben nach Artikel 3 Absatz 1 lit. i RTS SUB.

7.7 Hinweis zu Meldepflichten und Informationsregister

Meldepflichten, insbesondere bezogen auf das Informationsregister, den jährlichen Bericht an die zuständigen Behörden und die Meldung von beabsichtigten vertraglichen Vereinbarungen (Artikel 28 Absatz 3 DORA) sind nicht Gegenstand dieser Umsetzungshinweise.

8. Operative Informationssicherheit

In diesem Abschnitt werden die Anforderungen an Daten- und Systemsicherheitsmaßnahmen des Artikel 16 DORA und der Artikel 31, 34 und 35 RTS RMF im vereinfachten IKT-Risikomanagementrahmen denen der operativen Informationssicherheit der Kapitel 5 BAIT/VAIT gegenübergestellt.

Für den Bereich der operativen Informationssicherheit im vereinfachten IKT-Risikomanagementrahmen ist insgesamt festzustellen, dass der Detaillierungsgrad der Anforderungen vergleichbar mit denen in Kapitel 5 BAIT/VAIT ist.

Bisherige Anforderungen bleiben im Wesentlichen bestehen und werden teilweise detaillierter beschrieben. Lediglich der Schutz von Daten auch während der Verarbeitung ist eine wesentliche Neuerung.

Allerdings enthält der vereinfachte IKT-Risikomanagementrahmen Erleichterungen im Vergleich zum regulären IKT-Risikomanagementrahmen, der unter anderem deutlich mehr Vorgaben für Daten,- System- und Netzwerksicherheit sowie Anforderungen an IKT-Systeme fordert, die von IKT-Drittdienstleistern betrieben werden.

8.1 Schutz von Daten auch während der Verarbeitung

Artikel 16 Absatz 1 lit. c DORA und Artikel 35 lit. a RTS RMF im vereinfachten IKT-Risikomanagementrahmen stellen im Vergleich zum Kapitel 5.2 BAIT/VAIT höhere

[22] Vgl. Antwort der Europäischen Kommission auf die Q&A DORA030.

Anforderungen an den Schutz von Informationen. Darin wird gefordert, dass Daten entsprechend ihrer Kritikalität in allen Zuständen (Verwendung, Übermittlung und Speicherung) zu schützen sind.

Während die Anforderungen an den Schutz von gespeicherten Daten und während der Übertragung gemäß Schutzbedarf in Kapitel 5.2 BAIT/VAIT gefordert werden, stellt die Anforderung gemäß Artikel 35 lit. a RTS RMF an einen Schutz von Daten während der Verarbeitung ein Novum dar, welches mit einem erheblichen Implementierungsaufwand verbunden sein dürfte.

Ein Verfahren für den Umgang mit kryptografischen Schlüsseln sowie Maßnahmen zu deren Schutz zu etablieren, wie in Artikel 7 RTS RMF des regulären IKT-Risikomanagementrahmens gefordert, entfällt im vereinfachten IKT-Risikomanagementrahmen und ist bisher auch nicht Teil der Anforderungen der BAIT/VAIT.

8.2 Automatisierte Erkennung und Behandlung von Schwachstellen

Die automatisierte Erkennung und der Umgang mit Schwachstellen wird in Artikel 31 Absatz 3 und 34 lit. d und i RTS RMF im vereinfachten IKT-Risikomanagementrahmen geregelt. Dabei müssen Finanzunternehmen eine automatisierte Schwachstellensuche sowie entsprechende Patches zur Behebung der Schwachstellen sicherstellen. Dieses Vorgehen ist entsprechend des Risikogehaltes der betroffenen IKT-Assets durchzuführen. Explizite Anforderungen an die Dokumentation werden nicht gestellt.

Die aus Kapitel 5.3 BAIT/VAIT bekannten „Gefährdungen des Informationsverbunds" werden im vereinfachten IKT-Risikomanagementrahmen nicht über „potentiell sicherheitsrelevante Informationen" identifiziert, sondern über **„**anomale Aktivitäten" (Artikel 16 Absatz 1 lit. d DORA). Der Detaillierungsgrad der Regelungen ist vergleichbar. Unterstützt durch geeignete Verfahren, müssen hierzu anomale Aktivitäten und Verhaltensweisen bei kritischen oder wichtigen IKT-Vorgängen überwacht und analysiert werden. Tests dieser Maßnahmen werden durch Artikel 24 und 25 DORA sowie Artikel 36 RTS RMF definiert, sind aber nicht Gegenstand dieser Umsetzungshinweise.

Gemäß Artikel 31 Absatz 4 RTS RMF sind Alarmschwellen und -kriterien für die Auslösung und Einleitung von Reaktionsprozessen bei IKT-bezogenen Vorfällen festzulegen. Auch hier zeigt sich die Aktzentverschiebung von der Informationssicherheit zum IKT-Risikomanagement (Kapitel 4.7/4.8 BAIT/VAIT).

Entgegen den Regelungen des Artikel 12 RTS RMF des regulären IKT-Risikomanagementrahmens, werden für den vereinfachten IKT-Risikomanagementrahmen keine Vorgaben an das Logging gestellt. Auch in den BAIT/VAIT ist dieses Thema nicht explizit adressiert.

Der Vollständigkeit halber sei erwähnt, dass DORA umfangreiche Anforderungen an die Behandlung, Klassifizierung und Berichterstattung von IKT-bezogenen Vorfällen (Artikel 17-23 DORA) und das Testen (Artikel 24 und 25 DORA, Artikel 36 RTS RMF) enthält. Insbesondere die Anforderungen an die Erkennung von anomalem Verhalten geht über den

bisherigen, stark Use-Case getriebenen Ansatz von Kapitel 5.4 BAIT/VAIT hinaus. Die vorgenannten Artikel von DORA sind jedoch nicht Gegenstand dieser Umsetzungshinweise.

9. Identitäts- und Rechtemanagement – Einführung des „Need-to-use“-Prinzips

In diesem Abschnitt werden die Vorgaben zur Zugangskontrolle gemäß Artikel 33 RTS RMF im vereinfachten IKT-Risikomanagement denen des Identitäts- und Rechtemanagements in Kapitel 6 BAIT/VAIT gegenübergestellt.

Die Anforderungen an das Identitäts- und Rechtemanagement im vereinfachten IKT-Risikomanagementrahmen sind weniger detailliert als die in den BAIT/VAIT. In Titel III, Kapitel II RTS RMF entfallen die expliziten Anforderungen an das Identitätsmanagement.

In der Zugriffskontrolle sind gemäß Artikel 33 RTS RMF Verfahren für die Kontrolle des logischen und physischen Zugangs einzurichten, zu überwachen und regelmäßig zu überprüfen. Hier wird das „Need-to-know“- und „Least privilege“-Prinzip aus Kapitel 6.2 BAIT/VAIT um das „Need-to-use“-Prinzip ergänzt. Das neu eingeführte Prinzip spiegelt sich im Sparsamkeitsgrundsatz in Kapitel 6.2 BAIT/VAIT wider, sodass hier nicht mit erhöhten Aufwänden zu rechnen ist.

Weiterhin wird unter anderem gefordert, dass

- die Funktionstrennung gewährleistet wird,
- die Protokollierung von IKT-bezogenen Vorfällen (Artikel 34 Absatz 1 lit. f RTS RMF) durchgeführt wird und
- die Nutzerinnen und Nutzer der IKT-Systeme identifiziert werden.

Allerdings werden im Vergleich zu den BAIT/VAIT keine Berechtigungskonzepte oder deren Prüfung mehr gefordert, was Aufwände deutlich reduzieren sollte.